Crowell

CLIENT ALERT

NIST Seeking Input on Potential Cybersecurity Framework Update

March 10, 2022

The National Institute of Standards and Technology (NIST) has published an RFI (87 Fed. Reg. 9,579) seeking stakeholder input on two major cybersecurity fronts:

1. the "use, adequacy, and timeliness" of NIST's existing Cybersecurity Framework (CSF), and
2. current and anticipated "supply chain-related cybersecurity needs," for NIST's National Initiative for Improving Cybersecurity in Supply Chains (NIICS).

The RFI response deadline is April 25, 2022.

Regarding the CSF, NIST has asked organizations to identify the major benefits and drawbacks they have realized in implementing the CSF since its publication in April 2018. While NIST has yet to announce plans to formally update the CSF, NIST's RFI notes that since the CSF's publication, much has "changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce." Along the same lines, NIST also recognizes that there is an increased "availability of resources to help organizations better manage cybersecurity risk."

NIST has compiled a non-exhaustive list of possible topics to be addressed in stakeholder comments on the CSF. Primary subjects include the following:

- the benefits of the CSF and how to measure those benefits;
- challenges to using the CSF;
- areas of the CSF that should be changed or removed; and
- if NIST does change the CSF, would backwards compatibility problems arise.

NIST is also seeking stakeholder input on how organizations use the CSF with "other risk management resources," such as those published by NIST or other organizations. Topics in this category on which NIST is seeking input include:

- suggestions "for improving alignment or integration" of the CSF with NIST resources, such as the Risk Management Framework, Privacy Framework, and IoT Cybersecurity Capabilities Baseline;
- organizations' use of non-NIST frameworks together with the CSF;
- how to encourage international adoption of the CSF; and
- new terms or concepts for inclusion in NIST's Online Informative References Program.

Regarding the NIICS, NIST is seeking information, generally, on (1) what cybersecurity gaps organizations are encountering in managing supply chains, (2) how organizations have been addressing these gaps, and (3) the steps NIST could take to help organizations in this effort. NIST writes that stakeholder comments "will inform the direction of the NIICS," which the organization has explained is part of NIST's broader effort to fulfill the Biden administration's May 12, 2021, Executive Order (14028) on Improving the Nation's Cybersecurity. NIICS-related topics that NIST has identified for comment include:

- the major cybersecurity challenges of supply chain risk management that the NIICS might address;
- the approaches and tools that organizations currently use to manage cybersecurity-related risks in supply chains;
- present gaps in cybersecurity supply chain risk management, whether these appear in NIST resources or otherwise;
- how cybersecurity supply chain risk management could be addressed in an updated CSF.

RFI comments will inform NIST as it seeks to bolster the CSF and NIICS in response to significant developments in both the cybersecurity landscape and organizations' cybersecurity resource offerings since 2018. In particular, NIST's RFI targets stakeholder feedback on the interoperability of the CSF, and organizations' related, diverse needs in securing supply chains.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1.202.624.2615
Email: ewolff@crowell.com

Alexander Urbelis
Senior Counsel – New York
Phone: +1.212.895.4254
Email: aurbelis@crowell.com

Garylene (Gage) Javier, CIPP/US
Associate – Washington, D.C.
Phone: +1.202.654.6743
Email: gjavier@crowell.com

Paul C. Mathis
Associate – Washington, D.C.
Phone: +1.202.688.3432
Email: pmathis@crowell.com